Electronic Prescribing of Controlled Substances: The Physician's Perspective

Alan E Zuckerman MD FAAP
American Academy of Pediatrics
Georgetown University Medical Center
aez@georgetown.edu

- AAP represents 60,000 primary care pediatricians, pediatric medical sub-specialists, and pediatric surgical specialists who are dedicated to the health, safety, and well being of infants, children, adolescents, and young adults
- AAP cares about EPCS because of the importance of EPCS to children with ADHD – this is about Ritalin not Oxycontin
- AAP cares about electronic prescribing
- AAP wants to reduce the barriers to the increased use of health information technology
- AAP is participating in HL7, ASTM, CCHIT and HITSP
- Dr Zuckerman is a practicing academic pediatrician who is a member of NCPDP, CCHIT IOWG, and HITSP CE-TC

EPCS:
Overview of Physician Issues

- There is an urgent need for EPCS to drive eRx
- What security measures will physicians tolerate to get EPCS?
- Attractiveness of smartcards and PKI
- Unanswered questions about PKI
- Comparing provider level PKI and vendor level PKI
- Making DEA registration as easy as possible
- Linkage to the NHIN
- A phased roadmap to PKI

Urgent Need for Electronic Prescribing of Controlled Substances

- The greatest risk for electronic prescribing is that people will not use it!
- Not having EPCS is a hardship to physicians using eRx
- Not having EPCS is a barrier to getting more physicians to use eRx
- Patients are being deprived of important quality and safety benefits of eRx decision support and calculators
- The risks of fraud and abuse are greater in the paper system than in eRx today

What Will Physicians Tolerate For the Sake of Having EPCS?

- Physicians who currently use eRx would tolerate small increases in cost to get the benefits of EPCS
- Physicians who do not use eRx today want to keep the cost low
- CCHIT will begin certifying eRx as part of ambulatory EHR in May 2007 so EHR may become more important than eRx alone
- Physicians do not want separate systems for EPCS and non-controlled substances
- Physician will carry a smartcard, but not several different ones for different purposes
- Physicians will not tolerate biometrics or secure ID changing passwords because of the time factor
- Physicians do not like sole source vendor lock – they want multiple vendor options
- Enrollment and identification must be quick and easy

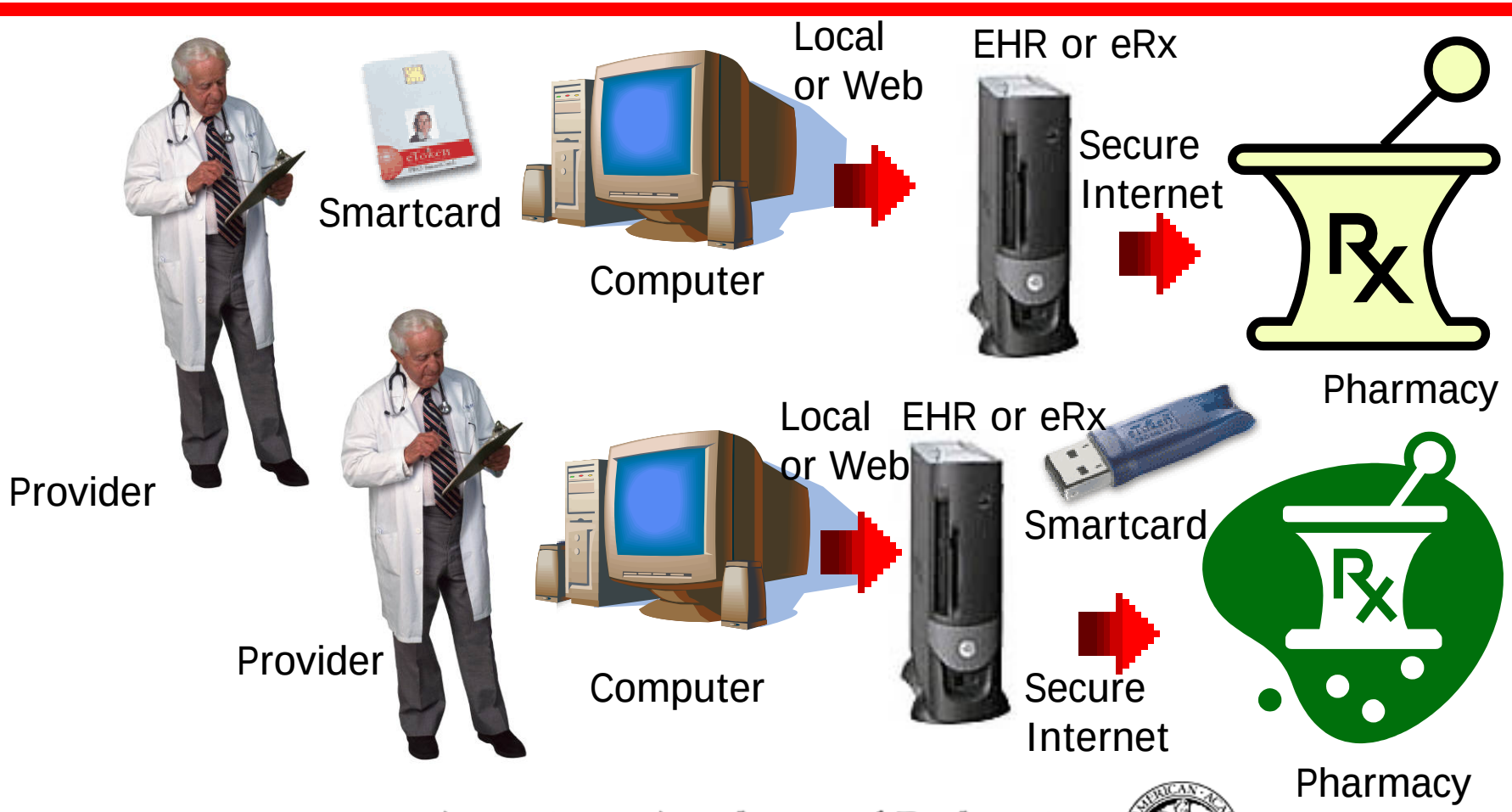
Attractiveness of Smartcards and PKI

- PKI adds 3 key features to electronic signatures
  - Third party user authentication
  - Document integrity checking
  - Non-repudiation
- A smartcard cannot be duplicated
- All critical processing takes place on the card
- Smartcards can be revoked remotely if lost or stolen
- Smartcards provide two factor strong authentication when used with the application password
- Smartcards now come in many form factors including USB smartcards and SD cards
- PKI can be used to protect the DEA number by encrypting the DEA number with the physician's public key

Unanswered Questions About PKI Use by Physicians

- Can we enroll large numbers of physicians and manage a large PKI outside of one enterprise? Limited experience with SAFE
- Can physicians really understand and accept PKI?
- A face to face identification step is necessary, but who will handle this function?
- Web Access and enrollment are essential
- Citrix Metaframe is used for some EHR and some use ASP
- Cell Phone / PDA will require SD cards
- Macintosh and Palm OS
- Will PKI middleware or drivers be in conflict with local HIPAA and other security systems
- Physicians will lose or forget their smartcards some of the time
- One solution is to move the PKI from the provider to the vendor

Comparing Provider Level PKI and Vendor Level PKI



American Academy of Pediatrics
DEDICATED TO THE HEALTH OF ALL CHILDREN™

Consider the Differences Between Provider and Vendor PKI

- Every provider must have their own smartcard
- Every provider must PKI enroll with the DEA
- The smartcard must be presented every time a prescription is signed
- Each provider has a secure digital identity and non-repudiation
- If the smartcard is not available, no prescriptions can be written

- Every EHR system and eRx system must have their own smartcard
- The EHR vendor or the eRx vendor must PKI enroll with the DEA
- The smartcard must remain in the system every time a prescription is transmitted
- Login to the EHR or eRx system is not changed from current practices
- Two factor authentication is optional, one smartcard can server many providers

Making PKI and Smartcards Easier for Physicians to Use

- Enroll only once every three years as part of DEA registration
- One fee plus the cost of the smartcard – today some hospitals provide smartcards for remote access
- Allow one smartcard to be used for many other purposes
- Instant web enrollment following the example of GeoTrust E-Mail certificates
- Choice of multiple smartcard vendors, form factors, and certificate authorities
- Basic cryptography that does not raise the cost
  - 1024 bit keys, RSA, SHA-1 not 2048 bit keys or SHA-256
- Self installing portable middleware and web applications

Critical Need to Coordinate With the Nationwide Health Information Network NHIN

- We must not allow two separate systems for physician digital identity and signature to operate side by side – EPCS and NHIN
- Electronic documents will require electronic or digital signatures on the NHIN including eRx
- The DEA could provide key services to the NHIN creating a national network of trust
- The NHIN could provide key security services for EPCS
- Today eRx is handled by separate networks and switches, in the future eRx should be part of the NHIN architecture
- EPCS and eRx issues must be part of the NCVHS hearings on NHIN functions scheduled for July 26-27, 2007

A Phased Roadmap to PKI for EPCS – Pilots are Essential

- Allow EPCS with same technology as eRx
  - As soon as possible, must resolve State Laws
- Require vendor PKI, node authentication and signed messages
  - Within 1 year
- Conduct real-world pilot studies of physician use of PKI and smartcards
  - Complete pilots within 2 years
- Harmonize EPCS with the NHIN
  - Within 3 years, only one identity for all purposes
- Set national standards for optional use of PKI digital signature
  - Within 4 years
- Revise interim standards for EPCS
  - Within 5 years, allow interim to become final if not revised